SERVICE DESCRIPTION
FORTIMAIL CLOUD

PUBLISHED: 2ND DECEMBER 2016

VERSION: 3.2

Contents

SERVICE DESCRIPTION
FORTIMAIL CLOUD

1. Disclaimer

This document is the copyright of Fortinet, Inc. ("Fortinet"), and is intended for internal use and Customer distribution only. Service in this document is defined as any combination of the various services outlined below and ordered by the Customer ("Service").

The purpose of this document is to provide a reference guide to the processes and procedures Fortinet employs when delivering the Service(s) and to define any service level metrics that Fortinet will endeavor to deliver against when providing FortiMail Cloud Email Security**.** This document defines any compensation ("Service Credits") that may be claimed by the Customer and provided in the event that Fortinet does not deliver according to the stated metrics.

This Service Description finally details Fortinet's and the Customer's key duties, obligations and responsibilities related to the provision of the Services described herein. This document forms part of the Agreement between the Parties.

2. Introduction

FortiMail Cloud Email Security is an independently validated and top-rated Secure Email Gateway solution delivering >99% catch rate, multiple layers of malware detection and an extremely low false positive rate. Fully managed by Fortinet, FortiMail Cloud Email Security allows the customer to focus on business goals by relying on a trusted security expert to manage this key infrastructure security component.

FortiMail Cloud is available in 2 different deployment options:

- **Gateway** — Route email to Fortinet where it is cleaned of malware and spam and forwarded onwards to existing customer mail servers.
- **Server** — Hosted email infrastructure and security with Fortinet while benefiting from Malware and spam protection as well as protection of sensitive information.

Additionally, for both deployments FortiMail Cloud there is a 'Premium' option, which adds Data Loss Prevention, Identity Based Encryption and Sandboxing. For the Server offering, the Premium service also adds additional mailbox storage.

3. Ordering

FortiMail Cloud can be ordered in the following formats:

Unit	Options	SKU
FortiMail Cloud – Gateway	*xx* depends on mailbox volume DD length of contract	FC-10-0VMxx-414-02-DD
FortiMail Cloud – Gateway Premium	*xx* depends on mailbox volume, DD length of contract	FC-10-0VMxx-415-02-DD
FortiMail Cloud – Server	*xx* depends on mailbox volume, DD length of contract	FC-10-0VMxx-416-02-DD
FortiMail Cloud – Server Premium	*xx* depends on mailbox volume, DD length of contract	FC-10-0VMxx-417-02-DD

Where DD is the term of the contract in months and xx is defined by the range of protected as shown below:

Number of Protected Mailboxes	*xx*
25-100	01
101-1,000	02
1,001-5,000	03*
5,001-10,000	04*
10,000+	05*

**Server Mode is only available up to 1,000 Mailboxes.*

4. Lead Time

The standard lead time for provision of the FortiMail Cloud service is five (5) working days from receipt of Provisioning information from the Customer. This may be extended if additional configuration and customization is required.

5. Service Prerequisites

5.1. Customer Infrastructure

The Service is available only if the Customer's email systems are permanently connected to the internet with a fixed IP address. Email systems connected to the Internet via dial-up, ISDN lines or using dynamic IP addresses are not supported.

Fortinet emphasizes that the configuration of FortiMail Cloud Services will be based entirely on the information provided by the Customer. Fortinet recommends that the Customer has an acceptable computer use policy (or its equivalent) in place governing its Users' use of email and that the FortiMail Cloud service is configured to supplement and support such a policy. In certain countries, it may be necessary to obtain the consent of individual personnel. Fortinet advises the Customer to always check local legislation prior as part of any deployment. Fortinet accepts no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of this Service.

5.2. Fair Use Policy

The Customer acknowledges that information sent to and from Customer will pass through the Service. Accordingly, Customer agrees to use the Service for legitimate and lawful business purposes only. Should Fortinet discover illegal activity, the service may be terminated without notice and the relevant authorities notified.
In the event that continued provision of the Service to the Customer would compromise the security of the Service, the Customer agrees that Fortinet may temporarily suspend the Service to the Customer.

5.3. Bulk Mailing Services

If the Customer is likely to be sending solicited bulk or marketing email, it is essential that this is communicated to Fortinet in advance otherwise it may lead to restriction or suspension of service. Sending of Unsolicited Bulk Email via the FortiMail Cloud service will result in immediate suspension of service.

The Customer agrees to indemnify Fortinet and its suppliers against, and hold Fortinet and its resellers harmless from, any and all claims, actions, losses, costs, and expenses Fortinet and its resellers may incur as a result of Customer's breach of this section.

6. Services

6.1. FortiMail Cloud – Gateway

The FortiMail Cloud — Gateway service provides cloud-based email security for customers with either on premise or third-party hosted email deployments. The service acts as an inbound and outbound gateway for customer email and cleans it of spam and malware before forwarding to its destination.

Feature	FortiMail Cloud Gateway	FortiMail Cloud Gateway Premium
Advanced multi-layer malware detection	●	●
Fully-managed service	●	●
Inbound and outbound filtering	●	●
Integration with customer LDAP	●	●
Secure message delivery (TLS)	●	●
Message tracking	●	●
Reporting	●	●
Data Leak Prevention		●
Identity-Based Encryption (IBE)		●
Cloud Sandboxing		●

6.2. FortiMail Cloud – Server

The FortiMail Cloud - Server is a cloud hosted managed Email Server solution combined with cloud-based email security. The service replaces the need to manage and maintain all on premise email servers with email being email hosting and security services being provided from the FortiMail cloud.

Feature	FortiMail Cloud Server	FortiMail Cloud Server Premium
Email hosting with POP3, IMAP & Webmail access	●	●
Advanced multi-layer malware detection	●	●
Fully-managed service	●	●
Inbound and outbound filtering	●	●
Integration with customer LDAP	●	●
Secure message delivery (TLS)	●	●
Message tracking	●	●
Reporting	●	●
Data Leak Prevention		●
Identity-Based Encryption (IBE)		●
Cloud Sandboxing		●
Mailbox size (per user)	5 GB	20 GB

7. Service Components

7.1. Malware

The Malware service component is provided through multiple layers of Anti-Virus detection methods including:

- FortiClient AntiVirus
- Dynamic Heuristics
- FortiGuard Outbreak Protection
- FortiSandbox (Premium Only, Optional)

This is then backed up by other methods including FortiGuard Outbreak Protection which utilizes big data analytics to analyses traffic flows across all Fortinet protected networks and identify new outbreaks “zero hour”.

The FortiMail Cloud Malware service operates to the following Service Targets:

- 100% Protection against known email viruses
- < 0.0001% False Positive Rate

This service will be configured to a ‘Best Practice’ configuration by the Fortinet assigned technical contact. Further configuration can be made in line with a Customer’s own requirements, for a full description of the configuration options available, please refer to the FortiMail Administration Guide.

7.1.1. Anti-Malware Actions

When a Protected Domain’s inbound email attachments is found to contain a Virus, by default, the message will be quarantined to the FortiMail Cloud System Virus folder. Optionally, the customer administrator can choose for a notification to be sent to the sender. Virus infected emails will be held for seven (7) days before deletion.

If a customer administrator chooses to release, or requests the release of a virus infected email, Fortinet will bear no responsibility for any consequences. Email will only be release to the original recipient or a named administrator.

Fortinet may at its discretion, refuse to release malware for security reasons.

7.2. Anti-Spam

Inbound Email to the Protected Domain will be scanned using a number of different detection methods to determine whether or not it is Spam. Each of these is summarized below.

The FortiMail Cloud Anti-Spam service operates to the following Service Targets:

- >99.5% Spam identification rate (95% for Email with Asian characters)
- <0.0003% False Positive Rate

7.2.1. FortiGuard Anti-Spam

FortiGuard AntiSpam Service collects millions of spam samples a day via Fortinet’s global spam trap network and spam sample submissions from Fortinet customers and partners. Meta-data on these samples is mined and bad IP addresses, content and spam object checksums and Uniform Resource Identifiers (URIs) are added to the FortiGuard database.

This method is enabled by default on all FortiMail Cloud Environments.

7.2.2. Behavioral analysis

Behavioral analysis encompasses a variety of methods to identify spam not caught directly by the FortiGuard AntiSpam service. By applying elements of heuristics and a fuzzy matching algorithm which compares spam recently detected (within the past 6 hours) by FortiGuard signatures on the device in question, behavioral analysis can detect fast changing spam samples. This method is useful to detect and prevent new “zero day” spam outbreaks and is enabled by default on all on all FortiMail Cloud Environments.

7.2.3. URI Filtering

In addition to the inbound Emails themselves, URIs embedded within the email body will be scanned and checked against the FortiGuard URI database. By default, emails in the following categories will be treated as spam and blocked:

- Security Risk:
  - Phishing
  - Malware
  - SPAM URLs

Additional URI categories are available for configuration on request. For a comprehensive list of the available categories, please refer to the FortiMail Administration Guide.

7.2.4. SPF and DMARK Check

Sender Policy Framework (SPF) records and DMARK use information published into a domains DNS server in the TXT record and allow domain owners to publish a list of IP addresses or subnets that are authorized to send email on their behalf.
The goal of this method is to reduce the amount of spam and fraud by preventing spammers to send spoofed email from third party systems. The service will be configured to use this information in the Spam decision process.

7.2.5. Sender Reputation

For incoming SMTP connections, the IP reputation of the sender is ascertained. Email originating from a disreputable source who have been seen to behave poorly (sending spam or performing directory harvesting attacks) will be slowed down and potentially blocked to minimize system impact.

7.2.6. Anti-Spam Actions

Where an Email is detected as spam, there are multiple anti-spam actions that are available to the Customer.

- Tag suspected email within the subject line
- Tag suspected email within the header
- Quarantine email to the users personal quarantine
- Reject suspected email
- Delete suspected email

As individual Customer organizations can have widely varying requirements for the proper action to take with spam content, Fortinet will require the customer to identify the appropriate actions when provisioning the Service.

7.3. Email Continuity

The FortiMail Cloud Platform provides a mechanism for Email Continuity should the customer Email server be unreachable. When attempting to deliver mail, should the FortiMail Cloud platform fail to contact a mail server, it will 'spool' the Emails, holding them until connection can be made once again.

The FortiMail Cloud Platform will hold Email for up to 5 days from time of receipt before discarding.

7.4. Premium Services

The following service components are only applicable to customer's who additionally utilize the 'Premium' options described above. As with other components, for full detail of the configuration parameters of these components, please refer to the FortiMail Administration Guide.

7.4.1. Data Leak Prevention

Data Leak Prevention (DLP) on FortiMail Cloud enables customers to identity particular file types, message contents or other criteria, and block them from being sent to external parties. When enabled, policies are configured that enable the FortiMail Cloud platform to identify traffic types the organization wishes to protect, and block these from being sent.

For full details of the configuration options of this service, please refer to the FortiMail Administration Guide.

7.4.2. Identity Based Encryption

IBE allows FortiMail Cloud to deliver confidential and regulated email securely. When enabled, IBE will 'capture' Email that meets defined policies, and send a HTML notification to the recipient via separate Email detailing instructions to retrieve their message.

Policies can be defined based on sender, recipient, or content, and allow a customer to ensure that potentially secure content is only viewed in a secure fashion.

- Policy-Based Encryption:
  - Automatically encrypt messages for compliance, based on content or recipient
- Push or Pull Mode:
  - Use Push, Pull, or a combination of modes to meet requirements

For full details of configuration options of this service, please refer to the FortiMail Administration Guide.

7.4.3. FortiMail Cloud Sandboxing

Today's most sophisticated cybercriminals are increasingly using 0-day threats in an attempt to bypass traditional anti-malware solutions in order to deliver advanced persistent threats deep within networks. These highly targeted attacks evade established signature-based detection by masking their malicious nature in many ways such compression, encryption, polymorphism.

When integrated with FortiSandbox Cloud, FortiMail queues emails containing suspicious content whilst the attachments and URLs are inspected for threats. Suspicious codes are subjected to multi-layer pre-filters prior to execution in the virtual OS for detailed behavioral analysis. The highly effective pre-filters include screening by the AV engine, queries to cloud-based threat databases and OS-independent simulation with a code emulator, followed by execution in the full virtual runtime environment. Once a malicious code is detected, the threat containing is quarantined preventing propagation into the network.

7.5. High Availability

Fortinet is responsible for the provision of High Availability configurations based on the number of Mailboxes deployed, within the Availability Target defined in 10.4, below. As part of the standard configuration, for deployments of 1,000 Mailboxes and above, High Availability pairs of virtual instances will be deployed. For deployments below this threshold, single virtual instances will be deployed.

This may be subject to alteration where specific customer/ configurations demand it.

8. Responsibilities & Access

The following table describes the responsibilities for parties in providing the FortiMail Cloud Service:

Action	Fortinet Responsibility	Customer Responsibility
Provision, Maintenance, Patching & Upgrades of the FortiMail Cloud Platform	Executes	
Provision of Service Components with default configuration settings as detailed in this Service Description	Executes	
Creation of initial administration accounts	Executes	
Creation of further administration and user accounts		Executes
Further configuration of profiles and settings to customize environment to customer needs.	Advises	Executes
Ongoing operational management of configuration		Executes
Provides support information necessary to interpret & resolve incidents	Advises (May Execute on request.)	Executes
Implements corrective changes to configuration to resolve and mitigate incidents	Advises (May Execute on request.)	Executes

9. Maintenance Windows

9.1. Planned Maintenance

"Maintenance" means periods of maintenance for which the Customer has been given forty eight (48) hours prior notification by Fortinet and which may cause disruption of Service due to non-availability of sections of the FortiMail Cloud infrastructure. Planned Maintenance shall not accumulate to more than eight (8) hours per calendar month and shall not take place between 8am and 6pm in the time zone in which the infrastructure is located.

Wherever possible, Planned Maintenance will be carried out without affecting the Service. This will generally be achieved by carrying out Planned Maintenance during periods of anticipated low traffic and by carrying out Planned Maintenance on part, not all, of the network at any one time. During Planned Maintenance periods the traffic may be diverted round sections of the network not undergoing maintenance in order to minimize disruption to the Service.

9.2. Emergency Maintenance

On rare occasions, emergency maintenance may be necessary and may be likely to affect the Service, Fortinet will endeavor to inform the affected parties soon as possible and in any case within one (1) hour of the start of the emergency maintenance.

10. Service Level Agreement

10.1. Terms of Agreement

This Service Level Agreement ("**SLA**") is provided by Fortinet and applies specifically to the Services indicated, as described in the Order documentation

10.2. General Terms.

The customer agrees to correct problems and to attempt to minimize the recurrence of problems for which the Customer is responsible that may prevent Fortinet from meeting the service level guarantees.

All Service Level calculations will be based from the point a service ticket is raised with Fortinet. Requests for customer support received by other means other than telephone or request ticket (for example, by fax, SMS, instant messaging, etc.) will be excluded when calculating service levels.

Fortinet shall not be liable in contract and tort (including negligence) howsoever arising out of or in connection with a failure of the Service, (including any collateral contract) for any:- (a) indirect, special or consequential loss of damage; or (b) loss of profits, business opportunities, revenue, anticipated savings; wasted expenditure, goodwill or for any loss or corruption or destruction of data to detect spam, pornographic images or specific content, or for wrongly identifying an email suspected as being spam, pornographic or containing specific content, which proves subsequently not to be so.

Furthermore, the Customer shall indemnify and keep Fortinet indemnified against any and all costs, claims, losses, liabilities, proceedings and expenses (including legal fees) which are brought or threatened against Fortinet by any person that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any item suspected as being or not being spam, pornographic or containing specific content

10.3. Exceptions

Fortinet excludes responsibility for meeting any service levels to the extent that meeting the service levels is affected by the following items:

i. if the Customer is in default under the Agreement;
ii. in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
iii. in the event that the Service is disrupted due to unauthorized user changes;
iv. in the event that the Service is unavailable due to Customer-initiated changes whether implemented by Customer or Fortinet on behalf of Customer;
v. in the event that the Service is unavailable as a result of the Customer exceeding system capacity;
vi. in the event that the Service is unavailable due to the Customer's failure to adhere to Fortinet implementation, support processes and procedures;
vii. in the event that the Service is unavailable due to the acts or omissions of the Customer, its employees, agents, third party contractors or vendors or anyone gaining access to the Fortinet network; or to the Customer's website at the request of Customer;
viii. in the event that the Service is unavailable due a Force Majeure Event;
ix. in the event that the Service is unavailable due to any violations of the Acceptable Use Policy defined above;
x. in the event that the Service is unavailable due to any event or situation not wholly within the control of Fortinet;
xi. in the event that the Service is unavailable due to the negligence or willful misconduct of the Customer or others authorized by the Customer to use the Services provided by Fortinet;
xii. in the event that the Service is unavailable due to any failure of any component for which Fortinet is not responsible, including but not limited to all Customer-provided or Customer-managed electrical power sources, networking equipment, computer hardware, computer software or email content;
xiii. In the event that the Service is unavailable due to any failures that cannot be corrected because the Customer is inaccessible. It is the Customer's responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details.

10.4. Service Level Guarantees

The FortiMail Cloud Service is provisioned under the following Service Level Guarantees:

- 99.999% Service Availability
- 100% Clean Email Delivery (within the Service Availability Guarantee)
- Average Email Scanning Time < 60 seconds.

10.5. Service Level Credits

If Fortinet fails to deliver the stated service level, Fortinet agrees that the Customer shall be entitled to receive, in lieu of all other remedies available to the Customer, Service Credits as set forth in this section against the Fees owing to Fortinet under the Agreement.

There are no Service Credits available for the FortiMail Cloud Service.

11. Liability

NO ANTI-SPAM OR ANTIVIRUS SOFTWARE CAN GUARANTEE A 100% CATCH RATE AND THEREFORE FORTINET CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT SPAM OR MALWARE OR FOR WRONGLY IDENTIFYING AND AN EMAIL AS SPAM OR ATTACHMENT AS MALWARE WHICH SUBSEQUENTLY PROVES NOT TO BE AS SUCH.

FORTINET EMPHASIZE THAT THE CONFIGURATION OF FORTIMAIL CLOUD IS ENTIRELY IN THE CONTROL OF THE CUSTOMER. FORTINET RECOMMEND THAT THE CUSTOMER ADHERES TO THEIR PUBLISHED AND AGREED COMPUTER ACCEPTABLE USE POLICY (OR ITS EQUIVALENT). IN CERTAIN COUNTRIES IT MAY BE NECESSARY TO OBTAIN THE CONSENT OF INDIVIDUAL PERSONNEL PRIOR TO DEPLOYING EMAIL INSPECTION SERVICES.
FORTINET CAN ACCEPT NO LIABILITY FOR ANY CIVIL OR CRIMINAL LIABILITY THAT MAY BE INCURRED BY THE CUSTOMER AS A RESULT OF THE OPERATION OF EMAIL INSPECTION.